WHAT IS CLAIMED IS:

1. A method for communication of messages in a secure manner in a communication environment which is subject to compromise, the method comprising:

a. providing an escrow agent, wherein said escrow agent generates a pair of keys comprising a public key and a private key;

b. causing said escrow agent to communicate said public key to all parties within a communication system to be used to support secure communication;

c. extracting at each party a common benchmark;

d. agreeing among each party on a starting interval key referenced to said common benchmark;

e. causing each party to generate iteratively a next interval key independently of each other party but with reference to an interval index, wherein said interval key is encrypted by said public key; thereafter

f. initiating a secure communication between or among parties using reference to said interval index and without communicating or exchanging their respective interval keys;

g. causing each party to a secure communication to encrypt a message to be secured using the common interval key independently computed based on said common interval index; and

h. causing said encrypted message to be communicated within said system such that said encrypted message can be decrypted using said common interval key.

2. The method according to claim 1 wherein said parties exchange their respective interval indexes and wherein the parties with the older interval indexes advance their interval index and compute said interval key corresponding to the latest interval index.

3. The method according to claim 2 wherein each party destroys each prior interval key after a new interval key is generated so that an older interval key cannot be recovered.

4. The method according to claim 1 wherein said interval index is not communicated to said escrow agent.

5. The method according to claim 1 wherein said starting interval key is not communicated to said escrow agent.

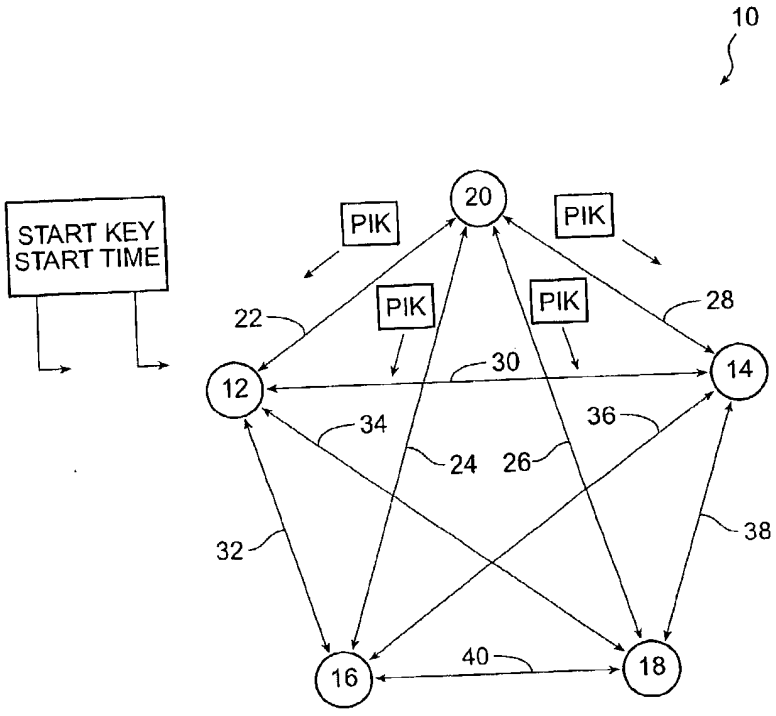
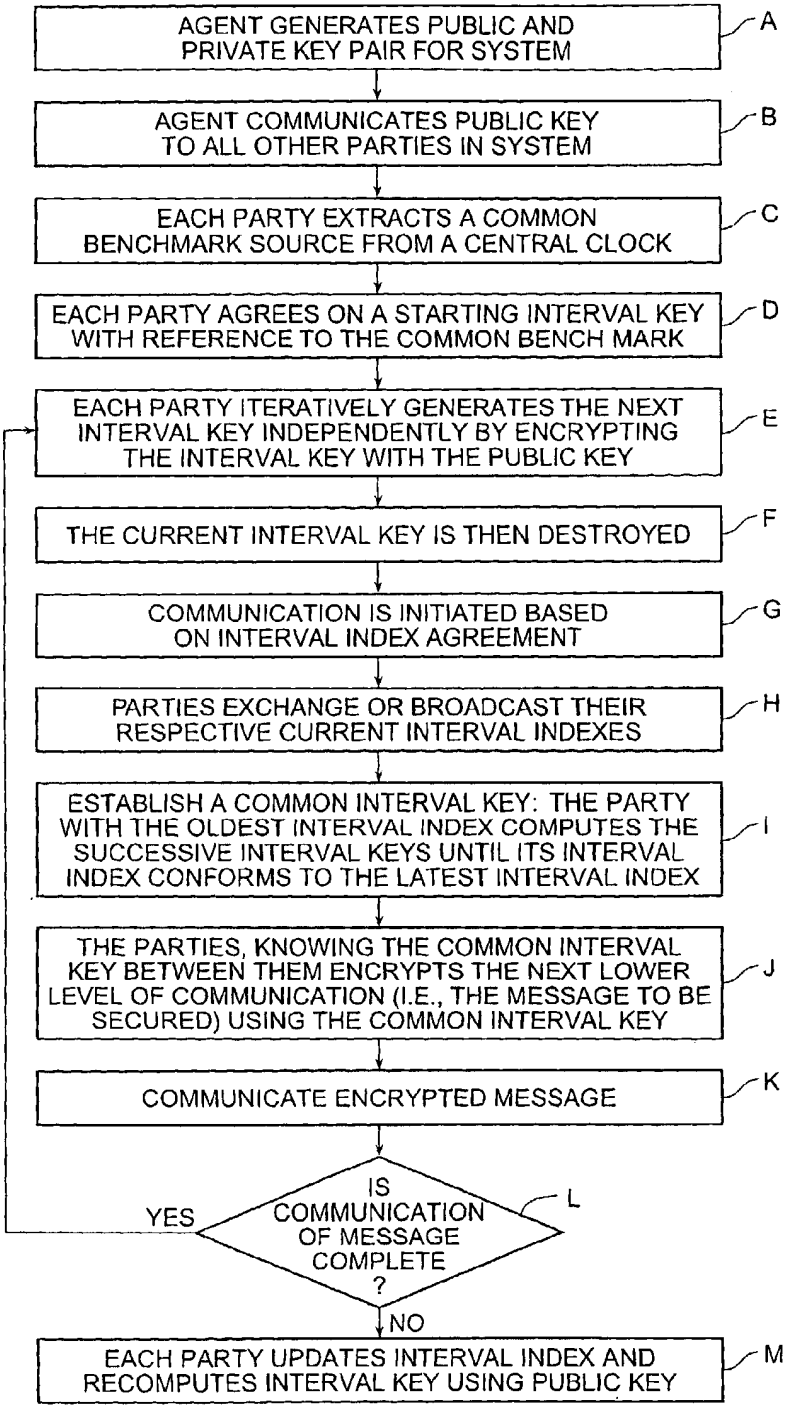


FIG. 1



(not interval keys)

FIG. 2